SSOAR

Open Access Repository
www.ssoar.info

Internet Shaping Freedom of Expression: Freedom Shaping Regulation

Singhm, Sumanjeet

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Singhm, S. (2017). Internet Shaping Freedom of Expression: Freedom Shaping Regulation. *Media Watch*, *8*(3), 157-176. https://doi.org/10.15655/mw/2017/v8i1/49014

Nutzungsbedingungen:
Dieser Text wird unter einer CC BY-NC-ND Lizenz (Namensnennung-Nicht-kommerziell-Keine Bearbeitung) zur Verfügung gestellt. Nähere Auskünfte zu den CC-Lizenzen finden Sie hier:
https://creativecommons.org/licenses/by-nc-nd/4.0/deed.de

Terms of use:
This document is made available under a CC BY-NC-ND Licence (Attribution-Non Comercial-NoDerivatives). For more Information see:
https://creativecommons.org/licenses/by-nc-nd/4.0

gesis
Leibniz-Institut
für Sozialwissenschaften

Mitglied der
Leibniz-Gemeinschaft

© *Media Watch* 8 (2) 157-176, 2017
ISSN 0976-0911 e-ISSN 2249-8818
DOI: 10.15655/mw/2017/v8i2/49014

Internet Shaping Freedom of Expression; Freedom Shaping Regulation

SUMANJEET SINGH
Ramjas College, University of Delhi, India

Recent years have seen a sequence of "moral panics" regarding accessibility of information on the internet and its exercise for criminal/harmful activity. Such problems and wider availability of internet raises the public policy concerns among governments over whether the internet should be regulated or not. Some believe it should not, considering that internet regulation will discourage what really internet is purported to encourage i.e. 'free flow of information'. They see internet regulation as a potential threat to the 'freedom of expression', which is possibly one of the most prominent aspects that are instrumental in the growth and popularity of this technology. On the other hand, the others who are against the free access of internet underscores the danger of problematic content and illegal activities on the internet. They claim that much of these activities and content are illegal in most jurisdictions. Adding to this, unrestricted right to freedom of speech and expression may possibly threaten other's rights. Thus many government organizations and internet users call for the regulation of internet. In this backdrop, paper revisits relevant literature and attempt to respond to the contentious problem of internet regulation. In this process, the paper also examines the experiences from several countries grappling with the problem of internet regulation. It concludes that any regulation on the internet has to be multi-faceted, culturally sensitive, and globally coordinated.

Keywords: Internet, regulation, governance, freedom of expression, access, digital

The internet is one of the most important driving forces behind the proliferation of the modern civilization. From its initial use for communication in military by the United States to its innumerable uses for various purposes worldwide, it has come a long way; and is here to stay as it has emerged as one of the most potent tools of ICTs. It enables interactive communication with less impedance created by distance, time, or choice of medium and reduces the cost of coordination, communication and information processing[1]. Despite the economic downturn, the use of the internet continues to grow worldwide. According to an estimate of ITU, in July 2016, the number of internet users worldwide reached 3.42 billion (meaning an internet penetration of 46.1 per cent), up from 394 million in 2000 and 1 billion in 2005. The number of internet users in the world is all set to cross a thumping 3.6 billion mark in early 2018 with nearly 50 per cent penetration. Thus, from the above data it can be concluded that the growth rate of internet surpasses that of any previous technology.

Correspondence to: Sumanjeet Singh, Department of Commerce, Ramjas College, University of Delhi, Delhi-110 007, India. E-mail: sumanjeetsingh@gmail.com

The ever increasing automation user base interacts with the system in umpteen ways. Generally people use it as a medium to connect or reconnect with acquaintances, for sharing files, recreational purposes, education, research and lots of other multitudinous productive activities. It has also become an important instrument to empower the poor people in developing countries (Panos, 1998; Avgerou, 2001 & Walsham, 1993). Various studies revealed that poor have experienced the benefits of internet in the form of increased income, improved health care, better educational prospects and training, access to better job opportunities, higher engagement in government services, frequent and better quality connection with family and friends, enterprise development opportunities, increased agriculture productivity, et al [2]. Not just individuals, but, the business populace is using internet and its enabled technologies like e-commerce as a part of their business strategy. As a result, more and more business activities are shifting from traditional commerce to internet commerce. Further at the economic front, it has the potential to increase GDP, stimulate economic growth and employment in developed as well as developing countries. It also allows the market agents (both buyers and sellers) to interact more effectively and efficiently by creating new market opportunities and has also impacted the costs of many kinds of market interaction to plummet (Sumanjeet, 2008).

Further, the issue of transparency is easier to manage with the internet, which results in monetary savings in addition to stakeholders' confidence in the socio-economic development process and system. In addendum, there are a number of things which can be put to use to help the web make a difference: be it donating money to charities via click through, providing aid to the local community, including financially and socially ostracized people (financial and social inclusion), or to raise our voice on sensitive issues by signing online petitions. Thus internet and its enabled technologies have become a driving force of modern civilization and offer many opportunities to those who are brave enough to seize them. As a result, governments around are the world are embracing this technology with great zeal and they are busy in formulating the policies to promote the internet as a tool of good governance and delivering various public services through Internet (Sumanjeet, 2006).

However, a coin has two sides, on one hand if the internet is a usefully penny, on the other hand it has a capability to create chaotic scenarios which may be harmful to our existence. The internet not only creates barriers to the business, society and government, it also creates a thousand areas where crime, unlawful or terrorist activities can proliferate. With the growth of internet users, the opportunities to exploit loopholes in information security system are also multiplying, thence cyber crime is born. Criminals, hackers, crackers and even slapdash persons without wrongful intent, can create stern problems through maltreatment of the internet's capabilities. Online financial fraud, data theft, viruses, breach of secrecy and privacy, denial of access, theft of services, copyright infringement and other related offences create losses up to billions of dollars annually[3].

Added to these, in the recent years a series of "moral panics" with respect to the accessibility of information on the internet and its use for criminal and harmful activity has been observed. These comprise of: the availability of sexually explicit material, the mis-utilization of the internet by pedophiles to distribute child pornography, the use of the internet by Neo-Nazis and other racist groups, the accessibility of hate speeches and bomb-making instructions and the use of encryption technology in order to safeguard private communications by terrorists and organized crime (as cited in Ellison and Akdeniz, 1998). One can take the example of terrorist organsaitons like Daish, Boko-Haram, Al-Quaeda, Hamas, Lashkar-e-Taiba, Hizb-ul-Mujehideen or ISIS. They use the internet to tap support and recruit the best users of internet technology for promoting their cause. Among these terrorist groups, the most proactive user of the internet is ISIS has launched several

social media campaigns and updates photos and statements to highlight its military strength. One video posted on June 17, 2014 viewed an ISIS member speaking in French and asking Muslims to support ISIS' cause online (Faisal, 2014). Online terrorists fundraising has become so common place that some organsaitons are able to accept the donations via popular online payment service 'PayPal' (Kaplan, 2009).

In short, the internet which was initially lauded, praised and seen as a blessing to the mankind as a wonderful and most potent medium of communication and the epitome of freedom of speech and expression has begun to show side effects that need stark attention. Such problems and wider availability of internet plainly raises public policy concerns among governments over whether the internet should be regulated or not. In this light, the present paper aims to investigate the rationality of internet regulation and analyze the approaches considered by various countries. For systematically study, the paper is divided into four sections. Section 1 presents an over-view of Internet and the purposes for which it can be used, while Section 2 discusses contentious side on Internet regulation. Detailed discussion on how different countries are regulating internet has been made in Section 3. Concluding remarks are presented in Section 4.

Debatable Perspective on Internet Regulation

In the current scenario, the debate on internet regulation can be seen from the viewpoints of two camps: Camp that support non-regulation of internet and camp supporting regulation of internet.

Views of camp that is against internet regulation: The camp that believes it should not be regulated, seeks that internet regulation[4] will discourage what really internet is purported to encourage i.e. *'free flow of information'.* For several years the internet has been an open and important source of information. It offers an unparalleled and massive amount of resources for information and knowledge and extricates new opportunities for expression and participation of people (Dutton *et al*.2010). It not only makes the movement and participation in traditional forms of protest-like street demonstration easier, but also helps these protests to break cross country barriers by effectively and rapidly spreading communication and mobilization efforts[5]. Online Social media like LinkedIn, YouTube, Twitter, Facebook, Instagram, WhatsApp etc. allow users to connect and communicate directly, and thus, potentially reduce the cost of coordination and promote collective action (Ruben 2015).

Evidently people throughout the world are using internet to accelerate their movements for equality, justice, social inclusion, strengthen transparency and better respect for human rights by enabling people to connect and exchange information instantly and by creating a sense of solidarity (Daniel 2014; Jeroen & Peter, 2010). The uprising of the Zapatista movement in 1994; anti WTO mobilization in Seattle in 1999; demonstration of Buddhist monk in Burma in September 2007; Jody William's global movement to eradicate landmines; *MoveOn.org,* an online petition initiatives,1998; *Twitter Revolution'* in Moldova; Tusnisian revolution, 2010; Occupy Wall Street, 2011; Arab Spring, 2011; Ukraine's Euromaidan Protest Movement 2014; #BringBackOurGirl 2014; #Ferguson 2014 that manifested the capability of Internet in terms of providing a common platform to share political views, along with organising and mobilising civil or political action are excellent cases to illustrate how the civil society has exploited internet to support their claim.

The passive use of internet technology as a means for a change has caused fear among those who wish to uphold the *status quo*. In this context, this terror of change

cannot justify censoring, monitoring, or blocking access to the internet. A stern regulation on internet will imply limited access to the broad source of information. A total capture or control by the authorities/governments or even other to top telecommunication players can lead to contravention of net neutrality and will reduce the usefulness of this technology (Uaddit, 2010); and it will be in contrast to the principle of net neutrality and will also permit certain websites to limit their content only to the paid customers. Sam Paltridge, an official in the OECD's (Organization for the Economic Co-operation and Development) directorate of science, technology and industry said (Eric, 2011):

> "We're trying to get the message across that if you hamper the flow of information; you are shooting yourself in the foot in terms of the economic benefits of the Internet,"

Regulation on internet technology will also tend to restrain the freedom of expression[6] which is a fundamental human right, which depicts on value of personal autonomy and democracy; and also closely connected to the freedom of thought and most importantly a precondition for individuals' self expression and self fulfillment. The right to self-expression also enables a free discussion about political, social and moral values and motivates artistic and scholarly endeavor free of inhibitions (as cited in Rikke, 2000-01). Freedom of expression can be termed as one of the most driving aspects that are instrumental in the success and popularity of this medium (Manohar, 2011). This logic and statement basically refers back to the origin of the internet. In fact, the principle of freedom of expression is embedded in the internet's robust architecture. A famous aphorism of Electronic Frontier Foundation (EFF) co-founder John Gilmore is that (as cited in John 2013):

> "The Net interprets censorship as damage, and routes around it. The Internet not only provides universal access to free speech, it also promotes the basic concept of freedom of speech. If you believe that there is an inherent value in truth, that human beings on average and over time recognize and value truth, and that truth is best decided in a free marketplace of ideas, then the ability of the Internet to promote freedom of speech is very important indeed[7]"

Any method intent to control internet content corresponds to a contravention of the people's right to freedom of expression and that such a right is absolute. It is not alluring to sacrifice freedom of expression so that parents do not have to monitor their children's internet usage. In this context Roger Darlington (2009) argued that:

> The Internet is a 'pull' not a 'push' communications network. This argument implicitly accepts that it is acceptable, even necessary, to regulate content which is simply 'pushed' at the consumer, such as conventional radio and television broadcasting, but suggests that it is unnecessary or inappropriate to regulate content which the consumer 'pulls' to him or her such as by surfing or searching on the Net.

In its consensus resolution A/HRC/20/8 (2012), the United Nations Human Rights Council (UNHRC) affirmed that the "same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice". There are several other human rights that are central in the framework of internet such as right to education, to take part in public affair, gender equality etc. As stated in Article 26 of the Universal Declaration of Human Rights (UDHR): Everyone has right to education. Everyone has the right to be educated

about the internet and to use the internet for education. Article 25 of International Covenant on Civil and Public Rights (ICCPR) provides that every citizen has the right and opportunity to take part in the conduct of public affairs, directly or through freely chosen representatives. This also applies to the internet public policy decisions, by virtue of the principle that offline rights apply equally online (as per Article 19 of the Universal Declaration of Human Rights).

The Tunis Commitment (2005) acknowledges that- full participation of women in the information society is necessary to ensure the inclusiveness and respect for the human rights within the information society. Beyond this, it is frequently stated that countries with a liberal and open environment regarding internet (which believe in securing the online human rights), experience greater economic benefits than those countries in which the internet is overly regulated (as cited in Daniel, 2014). As mentioned by Hill (2014), economic rights such as 'the right to standard of living adequate for the health and well being of himself and of family, including food, clothing, housing medical care, education and other necessary social services cannot be fully realized in today's world unless all people have equal influence in the development process and use of the internet. This is because the various aspects of life are now impacted by the automation technology which is spreading its wings to the farthest corners.

Then there is the pragmatic argument against internet regulation which has two strands. Firstly, it's naive to think that one country can attempt complete regulation. As Internet has global usage, so for the regulation to be effective, it needs to be global as well. Apart from being asinine, this type of regulation would also have many negative impacts on the country economically as the sites involving electronic commerce, which are of great economic use to country, might move elsewhere (UNRC, 2011). The other strand is that any material that is legal on the site of one country might be illegal in the other. As e-commerce go beyond the geographical boundaries, concepts like the transactions and consumption places become irrelevant. Therefore, it is often tricky to decide national jurisdiction and revenue rights especially in the case of digital services and products. Thus, how to tax e-commerce transactions have various intrinsic complications related to, for example, the verification of the location, identity and residence of seller or purchaser over the internet. As there are difficulties in the verification of the identity of the buyer, the seller and various parties related to the transaction, it becomes nearly impossible to enforce liability, collect the tax, and allocate it jurisdictionally, with all this happening up in the air (National Research Council, 2001).

As a basic conception about the internet is that it is a networked commodity, which denotes that its value swells with its extent. For example, increase in the number of internet users offers huge opportunities for the online businesses. In fact, this is one of the important reasons why many traditional companies are shifting their marketing battle from traditional media to electronic media. Any obstacles in this network will scrap it, and condense the overall value of the network. It can however be argued if the size of the network needs to increased, then there needs to be sufficient private gain for the network provider. Enforcing something like net neutrality, could come against that. This logic is certainly used in many other networks including that for cable TV (Srinath, 2015).

Added to this, whenever there's an argument related to the regulation of any technology, it is generally assumed to be a private good, so the regulation of it by the government becomes questionable. This conceals the truth that technology is more often a product of public and private collaboration (Anthony, 2013). Finally, and importantly, there is the argument due to its features like its ambiguity, iniquity, anonymity, vast reach and high monitoring potential, the Internet cannot be effectively regulated. Practically,

complex digital system aside, even making an ordinary physical space safe and secure is a challenge these days. The internet is not a single thing. It is a set of communication standards and network of computers generally portrayed as anything, anytime and anywhere that provides a wide range of communication and easily crosses borders in a way that makes intellectual property rights (IPRs) laws look trifling.

The views of the camp supporting internet regulation: On the other hand, the camp that is against the free access of internet underscores the danger of problematic contents and illegal activities on the internet. Financial frauds, false information, instructions regarding explosives, certain forms of gambling, harassment, cyber terrorism, child pornography, excessively violent material, illegal transactions, theft of resources, suicide assistance, defamatory allegations, cybers talking, prostitution, breaking and entering, copyright infringement, domain name disputes, money laundering, and many other exact or approximate electronic analogs of improper behavior can be found on the internet[8]. But one of the most dreadful use of internet (websites, message board, e-mail, real time web cameras, streaming video and through file sharing) is for child sexual exploitation. In a study conducted by iSafe Foundation (2014) at least 52 per cent teens have been bullied online. The study also reports that 35 per cent of those who witnessed bulling on social media sites have actually been threatened online, some more than once. Approximately 1 million children on Facebook were harassed in 2011 as reported by Consumer Reports. In most of these cases victims do not report to their parents and police. There is no political, ideological and financial justification for this crime.

As the real world grows more liberal of differences and disagreements, the virtual world grows with hatred (Howard 2009). Study of Jason et al 2015 revealed that increased internet access led to a rise in racial hate crimes. Hate speech lies in a circuitous nexus with the freedom of expression[9], individual, association, group and minority rights as well as concept of dignity, religion, value, equality and liberty (Iginio et al., 2015). Hate is pervasive on the internet, and it takes many forms having anti-Semitic themes, hateful image, words, slogan, sentence, speech, racist propaganda, distorting history etc. Whatever be the form of hate crime-it is threatening communication and is contrary to the democratic principle. To take the hate speech tradition to a whole new level, internet users come up with hate speech sites representing bigotry opinions.. More than a thousand RSACi rated sites are operating in UK alone, and many others in Asian and Australia. In 2012, there were around 1007 hate groups in the U.S. including Anti-Immigrants, Anti-Muslim, Black Separatist, Christian Identity, General Hate, Neo Nazi, Holocaust Denial, Ku Klux Klan, Racist Skinheads, Ani-LGBT etc, according to Southern Poverty Law Centre (Mahapatra, 2014). Such speeches increase in magnitude when the appropriate action is not taken by the concerned authorities and due to internet's vast expanse, such views are communicated to a large number of people creating further ignition.

Online piracy is another problem for many artistic natured businesses. One credible study by the Institute for Policy Innovation pegs the annual harm at 12.5 billion U.S dollar in losses to the U.S. economy as well as more than 70,000 lost jobs and US $2 billion in lost wages to American workers. The most visible blow to copyrighted works was seen in the music industry. A study conducted by members of PRS for music, a non-profit agency, found that of the 13 million songs for sale online in 2008, 10 million never got a single buyer and 80 per cent of all revenue came from about 52,000 songs. That's less than 1 per cent of the songs (Michael, 2008). In 2010, global recorded music sales dropped by almost US$ 1.5 billion due to the continued surge in the digital piracy in the industry (Sweney, 2011). The height of the problem is evident from the Digital Music Report (2012). The report was

illustrated on the basis of research that was commissioned by Harris Interactive in UK which stated that 23 per cent of consumers regularly download music illegally using Google as their means to find the content. In New Zealand, a report by Ipsos MediaCT (August, 2011) also highlighted that search engines direct a considerable number of users to unauthorized sources. 54 per cent of users of unauthorized download stated search engines as to be their sole source to find music. In Ireland, this figure was 49 per cent (Ipsos MediaCT, October 2011).

Apart from music industry, the movies industry has also been affected with the online piracy; in fact pirating movies online is as popular as pirating songs and it hurts the film industry a lot more. The internet went all insane when Hugh Jackman's *'X-Men Origins: Wolverine'* was available online, a month before the scheduled release. The American war film *'Fury'* starring Brad Pitt was leaked online by a hacker attack group called Guardians of Peace. They also released four of other Sony titles. *'Hurt Locker',* a small budget war film was unable to rake in moolah due to piracy (Borkar, 2015). *'The Wolf of Wall Street*' was the most pirated film of 2014 with over 30 million illegal downloads (Borkar, 2015). If each illegal download of movie is equated with one movie ticket in monetary terms, it costs US$8.17, and the movie studio only has half the share in each movie ticket, that results in about $122,692,975 that was robbed from Paramount Pictures for just that one movie (Spangler, 2015). The Motion Picture Association of America discovered that piracy costs around $20.5 billion annually in US alone (Plumer, 2012).

Another major threats posed by the internet technology is breach of secrecy and confidentiality. Even top US companies including Wal-Mart, JP Morgan, Community Health System, The Home Depot, Neiman Marcus, Apple, have not been immune to cyber security breaches. E-Bay suffered largest data breach in 2014 with more than 150 million records comprised. And most recently, YAHOO has revealed that data related to more than 500 million user accounts has been stolen which is touted as one of the largest cyber security breaches ever. A hacker breached Sony's servers and leaker a wide range of data including internal documents of employees and actors, as well as copies of unreleased movies such as Annie, Mr. Turner, Still Alice, and To Write Love on Her Arms. This led to many theaters refusing to screen Sony's film (Kyle, 2015). In early March 2013, India's top military organization, the Defence Research and Development Organization (DRDO) was hacked by some Chinese hackers, which was touted to be amongst the biggest such security breaches in the country's history (Harris, 2013). The Pew Research Center's State of Cybercrime Survey (2014) has reported that the U.S. Director of National Intelligence has ranked cybercrime as the top national security threat, above terrorism, espionage, and WMDs (IAMAI 2013).

Extortion of data, data destruction, release of confidential information, demonstrated denials of service (DDoS), disrupting state infrastructure, and holding information ransom are some of the weapons in the array used global cybercriminals, along with stealing data being the most common one. (Clark, 2015). The cost of cyber crime for the global economy has been estimated at US $445 billion (£266 billion) annually. More than 800 million people during 2013 have been affected by cyber espionage resulting in the stealing of their personal information. Financial losses from cyber theft could cause as many as 150,000 Europeans to lose their jobs, according to a report conducted by internet security company McAfee (Williams, 2014).

Any society is entitled to protect itself by imposing the criminal law in relation to such online contents and activities just as scrupulously as it would if similar activity occurred off-line and, in a sense, this means regulation of the internet. A severe internet

regulation can help to retrain the numerous illegal activities over the net. Although there exists several commandments about child pornography or prosecutions of pedophiles, these issues are still raging on the internet. The censorship of web can block the access of such disturbing websites, regulate or even shut down some of these sites, and thus reduce the exploitation of internet users. Internet regulation will also lead to tougher policies over unjustified defamation. Internet regulation will also assist in preventing the large number of financial frauds, phishing, and many other illegal activities, which are possible because of the unregulated and unrestrained internet activities (Houng, 2011).

Further, there are regulations governing the content of television, radio, newspapers, magazines, movies and books, so why not the Internet as well? (Kenneth & Herman, 2008). Albeit, Internet is considered to be different from these mediums in some sense, but basically it is just another communication network. If any government takes the decision of not regulating the internet, effectively over time they are going to abandon the notion of content regulation. This camp also argued that an unrestricted right to freedom of expression would imperil the right of children to be free from abuse or molestation and the right to ethnic minorities to live their lives free of racial intimation and violence.

Moreover, some form of regulation over the Internet is generally favored by most the governments and politicians. In taking this view, it is clear that they have the support of consumers' group and users themselves. This development is actually in contrast with the technological and academic origins of the internet and with the convention of self-regulation and non-interference on the part of government.

Approaches towards Internet Regulation

From the above discussion it is clear that despite the fact that the Internet offers huge opportunities, there are several real reasons why the internet needs to be regulated in order to ensure the millions of people who use it for their personal, social and business lives are protected and such opportunities are utilised up to their maximum potential (Rose, 2012). Thus, instead of debating whether to regulate the internet or not, a more sensible question to ask should be what kinds of regulation are viable and desirable. To achieve an understanding of what can be done to address the downside of the internet, there is need to understand the nature of the internet related problems. Broadly, content related problems of internet *(nature of internet problems)* have been largely recognized and classified as illegal[10] and harmful contents. The illegal and harmful use of the internet involves a very wide range of issues including areas such as national security, child protection, economic security, racial discrimination, pornography, privacy protection, gambling, malicious hacking, unauthorized distribution of copyrighted works e.g. software or music, unlawful comparative advertisement, fraud, instructions of pirated credit cards, abusive form of marketing, sale of controlled drugs, libel, and information security. Indeed, it can be said that almost all aspects of societal activity are part of an analysis of the downside of the internet (Department of Justic, Equality and Law Reform, 2010). The European Commission in its 1996 communication on illegal and harmful Contents on the Internet stated that:

> "These different categories of contents pose radically different issues of principles, and call for very different legal and technological responses. It would be dangerous to amalgamate separate issues such as children accessing pornography contents for adults, and adults accessing pornography about children".

The difference between illegal and harmful contents is that the former is criminalized by national laws, while the latter is considered as offensive/disgusting, but certainly not criminalized by the national laws (Yaman, 2001).

In this sense, illegal contents/activities can simply be regulated by law or regulatory instruments. Therefore, *'command and control'* approach can be used as an instrument to regulate illegal activities/contents. But, in case of harmful contents/activities which is basically a behavioral problems (*e.g. excessive use of Internet)* cannot be regulated by law. For this purpose, *self regulation*[11] can be used as an instrument. Third, as all activities/ contents related to Internet are routed through Internet Service Providers (ISPs) and content providers, there is need to establish a system that will provide for the responsibility of those who are technically capable of controlling any uses which depart from those permitted by law. These approaches are discussed in more detail below.

Command and Control Approach

Many nations are striving to find ways of controlling the internet technology through introduction of new laws, or through the amendment of already existing laws. There is no all encompassing legislation in US which regulates and controls the collection, storage, transfer, or use of personal information on the internet. However, due to the development of new technologies, the response has been to enact laws designed to target specific issues on an ad-hoc basis (Palme 1998, US Legal, 2009). For example, the Communications Decency Act[12] (1996), which, among other things, wanted Internet Service Providers to ensure that "indecent" information, is not distributed to minors (Palme, 1998).

The Electronic Communication Privacy Act (ECPA), 1986 regulates intrusion into electronic communications and computer networks. Digital Millennium Copyright Act (DMCA) of 1998 govern the use of copyright material in the US, Child Online Protection Act (COPA), 1998 restricts access by minors to any material defined as harmful to such minors on internet. The Children's Online Privacy Protection Act (COPPA) 1998 regulates unfair and deceptive acts and practices with regard to the collection and use of personal information from and about children on the Internet. Children's Internet Protection Act (CIPA) was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the Internet (FCC 2016). The Unlawful Internet Gambling Enforcement Act[13] (UIGEA) enacted in 2006 that *"prohibits gambling business from knowing accepting payments in connection with the participation of another person in a bet or wager that involves the use of Internet and that is unlawful under any Federal or State law".*

In UK, many regulatory initiatives[14] have been taken up to deal particularly with the presence of illegal or harmful contents over the internet. Obscene Publication Act 1959[15], the Protection of Children Act 1978 were amended by Criminal Justice and Order Act 1994 to take into account new technologies like internet for offences like child pornography (EFA 2002). On September 1996, UK Government issued R3 Safety-Net action plan developed by UK ISP trade associations and agreed by Government involving industry establishment of complaints hotline and related take-down procedures for illegal Internet content, primarily child pornography (EFA 2002). In relation to cyber-stalking and harassment issues, the Protection of Harassment Act was enacted in 1997.

The Official Secret Act 1989 is applicable for publication of official secrets over the internet. Added to this, there are number of laws restrict the use of the Internet in the UK, including laws against possession of certain types of material, English defamation law and the Copyright law of the UK (Akdeniz, 2001). UK Parliament also passed the controversial

Digital Economy Bill on April 2010, which grants the UK government sweeping new powers to control access to the internet. The Counter Terrorism and Security Act was passed in 2015 to reinforce the capability of law enforcement agencies to investigate which device is responsible for sending a communication on the internet or accessing an internet communication service.

Internet is highly regulated in China due to a wide range of laws and administrative regulations. China's Internet control is considered as more widespread and more advanced than in any other country of the world. There are at least 12 different government bureaus which have some authority over the internet, including the powerful State Council Information Office, the Ministry of Public Security, and the Ministry of Information Industry, which is in charge of licensing and registration of all internet content providers (Open Net Initiative 2006). Chinese government has two main ways of controlling what its citizens see on the net: *'The Great Firewall'*, which is basically a system of limiting access to foreign websites, which started in 1990s, and the *'Golden Shield'*, a system for domestic surveillance set up in 1998. In extreme conditions, internet access may be cut off altogether, as happened for ten months in 2009, after insurgences in Xinjiang. In 2015, the Cyberspace Administration of China announced more explicit rules on internet regulation which mainly includes fines for publishing pornographic material, false information or rumors and maintains incomplete internet security system (Chin, 2015).

An attempt has been made by the Swedish government to regulate the Internet through the Data Act and the Bulletin Board System (BBS) Act. However, no specific law has been enforced that compels Internet service providers (ISPs) to block access to sites. ISPs collaborate with police on their own to block a centralized list of sites trafficking in child sexual abuse. Australia maintains the highest degree of regulation with regard to Internet policies as compared to any Western country. In the preceding few years, Australia has taken steps toward a nationwide mandatory Internet filtering scheme (Roy, 2002). Its neighbor, New Zealand, however maintains lesser restrictions on the Internet. (Open Net Initiative 2006).

Australia's constitution restricts the right to explicit free speech, and in fact contains a clause giving the Australian government ''communications power,'' which allows it to regulate ''postal, telegraphic, telephonic, and other like services,'' including the internet (Geraldine, 2000). As the constitution of Australia does not afford that power to the national government (Electronic Frontiers Australia, 2006; Open Net Initiative 2006), a number of state and territorial governments have passed legislation making the distribution of offensive material a criminal offence. Any material that is considered as "RC" (Refused Classification or banned) or "X18+" (hardcore non-violent pornography or very hardcore shock value) in Australia is not permitted to be hosted within Australia and considers such content "prohibited potentially prohibited" outside Australia; and most of the age-restricted content sites require the verification of the user's age before allowing access (ACB, 1995).

India, too is coping up in the race of using legislation to regulate internet contents. In June 2000, the Information Technology Act (IT Act 2000) was passed by the Indian government to provide a legal framework to regulate internet use and commerce, including digital signatures, security, and hacking. Under the act, it is illegal to publish obscene information electronically and police have the powers to search any premises without a warrant and can arrest individuals who are suspected to be violating the act. An amendment to the IT Act in 2008 strengthened government's authority to block internet sites and content and criminalized sending messages which were to be inflammatory or offensive (World CP,

2014; ACB, 1995). As of now, there is no law that prohibits viewing pornography. The Indian Penal Code (IPC) and the recent IT Act both prohibit the production and transmission of "obscene material". After the bombings in Mumbai in2008, the Indian authorities have augmented the internet surveillance and pressure on technical service providers, while publicly rejecting accusations of censorship (Kumar, 2014).

In Saudi Arabia, internet has been regulated through a single government control centered since 1999 when internet access was first made available. From this center, government blocks access to the internet content deemed unsuitable for the country's citizens, such as information considered sensitive for political or religious reasons, pornographic sites, etc (EFA 2002). In South Korea, "The Internet Content Filtering" law became effective in 2001. Singapore is well known country that blocks downloading of politically unacceptable information from the net. Computer Misuse Act was introduced in 1993 for computer related matters. Following the 2013 Singapore cyber- attacks, the Act was renamed to Computer Misuse and Cyber Security Act. On October 7, 2014, Remote Gambling Act was passed with intent to protect young and other vulnerable persons from being harmed or exploited by remote gambling.

Added to these, there are countries whose government are involved in active, invasive surveillance of service providers (online as well as offline), resulting in grave violation of freedom of information and human rights. Countries where internet is most controlled are: North Korea *(all websites are under government control)*, Burma *(authorities filters e-mails and block access to the sites of political opposition groups, organizations working for democratic change in Burma, and pornographic material)* , Cuba *(internet available only at government controlled access points)*, Saudi Arabia *(Saudi Arabia's already restricted cyberspace is now subject to new regulation that allows the state to directly administer and control internet content),* Iran *(bloggers must register at Ministry of Art and Culture)*, Tunisia *(the government filters all content uploaded and monitors e-mails)*, Vietnam *(it bans bloggers and users of social media from quoting, gathering, or summarizing information from press organizations and government websites)* and Turkmenistan where (government is only the internet service provider and it bans/blocks access to many sites and filters all e-mail accounts registered with Gmail, Hotmail and Yahoo).

Thus, all around the world, the phenomenon of internet regulation is on the rise since approximately 1995 as more and more countries implement such laws to address the problem of material that is illegal in their traditional (offline) laws, and also that is considered harmful or unsuitable for minors. However, intensity of regulation varies from country to country. In case of internet regulation most laws are useful at domestic level but ineffective in case of cross jurisdictional or cross border issues. Added to this the nature of material of principle concerned has also varied substantially.

Non-Regulatory Approaches to Content Regulation

A systematic, non-regulation based approach is essentially desirable because the alternative-reliance on overboard, highly intrusive regulation, with laws differing across the national borders-yield short term, often crisis driven, mostly ineffective solutions. Thus a broad range of non-regulatory mechanisms *(self regulatory*[16]*)* have been developed to assist in responding to and minimizing the use of harmful contents/activities (e.g. racist comments) content on the internet. These include hotlines, filtering[17], rating systems and education and awareness. Established and operated by a variety of organsaitons, hotlines serve as an interface between the net users, content owners and law enforcement

organsaitons/agencies. One of the most significant[18] European hotline associations is INHOPE[19] (Internet Hotline Providers in Europe). INHOPE is an active and collaborative network of 51 hotlines in 45 countries worldwide which deals with illegal and inappropriate content online and is determined to stamping out child sexual abuse from the internet. It has broadened its focus to the problem of racism (xenophobia) on the internet in recent years (Australian Human Right Commission 2002). As per the latest data being collected with respect to INHOPE, 98 % of all user reports to national hotlines are forwarded to law enforcement agencies within one day. Moreover, illegal content is deleted within three days in 91% of the cases. And there are over 500 000 reports made to European hotlines each year (EuroISPA 2015).

In the recent years, concerning the colossal availability of offensive material on the web, internet content rating systems are developing with broad support of government agencies and industry. Rating systems allow content creators and/or third parties to classify content. The Internet Content Rating Association (ICRA) is the most prominent rating association (Australian Human Right Commission 2002). Prominent rating systems currently in use include ICRA (which was RSACi), SafeSuri (developed by SafeSuri Corp) and NetShephered (based in Canda). ICRA and SafeSuri rely on self rating of internet sites by web publishers. By contrast, NetShephered conducts third party ratings of the sites.

Internet content can also be regulated through those technical approaches implemented at different levels of access to the network (known as filtering). Filtering can be used in different ways to block offensive materials: Browser based filters, E-mail filters, Client-side filters, Network based filters, Content limited ISPs and Search engine[20] filters. From UK and their web filters to "*the Great Firewall of China",* countries around the world the using filtering technology against the technology that blocks content tagged as illegal, harmful or offensive. Increasingly, many countries are deploying commercial filtering applications to filters such contents. Iran and China are excellent example which had "pervasive" political and conflict/security filtering along-with "substantial" internet tools for social filtering. Today, many governments are shifting from endemic blacklists of sites to filters towards the *"next generation filtering,"* which includes targeted surveillance and *"just in time"* filtering, or *"temporarily filtering"* content only when it is important (The Guardian, 2012).

The regulatory scheme in many governments emphasis on self regulation through shouldering the liability on ISPs through the development of codes of practices. Logically, these intermediaries have the necessary technical capacity to prevent the circulation of such communication[21]. As a result, in last decade many governments/organsaitons have lobbied with these intermediaries to compel them to police their network and content filtering, protocol blocking, blocking access to known infringe websites and implement anti-file sharing technologies. These lobbying efforts have met with some success. In June 2007, a Belgian court ordered an ISP to install filtering software to identify and block illegal file sharing of copyrighted music. In June 2013, the big four ISPs in the UK-BT, Sky, Virgin and TalkTalk had agreed to provide their customers with free parental controls which can be activated any time (Hirst, 2014). Recently, in GEMA (also known as German music rights group), Germany's Supreme Court ordered that an ISP can be required to block sites that infringe on copyrights.

In Australia, a regulatory regime for Internet Content was introduced in 1999. The regime places obligations on ISPs as well as Internet Content Hosts (ICHs). It also requires the development of industry codes of practice. In Singapore, all ISPs and Internet Content Providers are required to ensure that their content complies with the Internet Class License

and the Internet Code of Practices. The main concern of Singapore's Internet Codes of Practices is content such as those relating to public interest, race, religion, pornography and content harmful especially for children (MDA 2015). Australia has also developed codes of practices purely concerned with content regulation. In Ireland, the Code of Practice and Ethics developed by Irish Industry Association outline guidelines for ISP service to create, host, transmit material which is unlawful/ abusive/offensive/vulgar/defamatory/ calculated to cause unreasonable offence (ISPAI, 2002). In India, the "IT Rules 2011" adopted in April 2011, as a supplement to the Indian Information Technology Act 2000, pressurize ISPs for the removal of any material/content that is considered to be objectionable, specifically if its nature is "Defamatory," "hatful to minors," or "infringe copyrights". In 2015, Indian government (Department of Telecommunication) has ordered ISPs to block 857 porn sites. Earlier in 2012, 309 URLs were blocked by government relating to rioting and communal violence in North-East. In countries like China and Saudi Arabia, the internet content market is controlled through ISPs.

End-user education is another non-regulatory tool that can be utilised to combat racism on the Internet. In line with its emphasis on protecting children from harmful content, the Australian Broadcasting Authority has developed its "Cybersmart Kids Online" education tool for children (Australian Human Right Commission, 2002; Jawahitha and María 2010). Canada has also established not for profit organization called the "Media Awareness Network" Mnet, which provide parents and educators with practical information and hands-on activities to empower children to be "safe and savvy" users. Most of these are overviewed in the Safer Internet Action Plan (SIAP) developed by the EU as well as by the United Nations (Jawahitha & María 2010).

Self regulator approach is generally broad in scope and can include issues which cannot be included in regulations. In fact, a systematic Self-regulation and the support of public authorities are complimentary to each other, be it because of the fact that they simply do not interfere with the self-regulatory process, or that they support or ratify self-regulatory codes and give support through enforcement. Self-regulation is very limited as far as its achievements are concerned. The process can only help ensure that criminals cannot use the internet with impunity, but it cannot make sure that that the criminals such as child pornographers are punished for their offences. (Gütersloh, 1999; COPA Commission 2000; Marie & Yves 2002). Education and public information should be used as mediums to spread and raise mass awareness among users about self-regulatory mechanisms such as the means to filter, secure and block content, in order to protect it from going into the wrong hands, and to register complaints about internet content through hotlines.

Conclusion

There is no disagreement on the conjecture that internet is shaping freedom of expression by providing individuals new modes of imparting and seeking information; but it is trite but true that this freedom (free flow of information) has also raised the call for content regulation which aims to address potential risks that accrue with the free flow of information. In turn, better or worse, new situation leads to more rules. Evidently, despite the supposed confrontation; national law has been endorsed throughout the world. This shows that governments are indeed concerned about 'regulating' the cyberspace.

At national level, it is imperative for every government to decide whether to fight (certain) online materials such as pornography, hate speech etc. or allow it. Governments also have to consider which actor is best suited to implement the prohibition of certain

contents. The regulation of content at the level of an ISP maybe a viable option, but it is faced with its internal, double edged difficulties. On one hand, if customer puts up or transfer data that goes against the general government guidelines, the ISP can be held liable for non-removal of such information for a civil or criminal procedure. While if an excess restriction is imposed on the customers for the kind of information they publish, it might breach the contract they have with their customers. There may also be occasions where an ISP may not wish to be associated with certain material on its systems. The best safeguard to such a situation is for the ISP to have clear and absolute terms and conditions/ guidelines which also allow for the authorized removal of undesired contents.

Government regulation and self regulation have long been considered complimentary, instead of being mutually exclusive, by the policymakers in the dominant legal systems. Thus, regulation, as it has evolved to date, can be best described as complex tapestry of government regulation and self regulation. Putting pressure on the ISPs to resolve the content related problems should not be the way forward as it will only hamper the development and growth of internet.

As discussed in the paper, a nation has many territorial weapons to fight offshore internet transactions. But, for many reasons unilateral regulation of internet is not efficient including one that a territorial government cannot regulate offshore content producers beyond the nation's physical control[22]. Considering the global nature of internet, international law could be more efficient and suitable tool for regulation in some of the various internet related issues. However, how to formulate and enforce laws at international level remains a spiky issue. Added to this important issue about internet regulation is: *"Who is doing the regulation?"*, and more to the point: "do they have a right to do so, derived from the consent of those they are regulating?" There are internet regulation bodies[23] (i.e., The Internet Society, The Internet Architecture Board, Internet Engineering Task Force, InterNIC, People for Internet Responsibility (PFIR), ICANN.org) that work behind the scene to keep everything running semi-smoothly; but there is no central internet regulation body. In the absence of central internet regulatory body it is really difficult to set down certain standards that all governments must obey. As many countries are not happy with US-Centric model (intent is overwhelmingly Global North-based) of internet governance, there is a strong need to democratized governance and this can be done through using 'multi-stakeholder model' in which a nation state is recognized as the representative of its citizens.

Indeed, there are no technical or legal instruments that assurance hundred per cent control over the internet. As the approaches discussed above show, attempts to regulated internet may result in little success, while damaging the repute of nation all over the world. What can be lucidly stated is that any form of regulation on the Internet needs to be multi-faceted, considering cultural sentiments, and globally coordinated. The global nature of the internet and the current requirement to deal with the inappropriate content being posted on Internet has resulted in new the formulation of new approaches to deal with such problems. A new partnership approach between the ISPs and the law enforcement agencies is predicted to be the best way, which would not only address criminal content and criminal activity over the internet, but also improve law enforcement techniques in relation to internet-related crimes (Akdeniz, 2001). In the end, it can be stated that upcoming advances in internet regulation would be shaped by the ability of policymakers to accept a new model of regulation that makes use of tools quite different from the still overriding and traditional model of '*command-and-control approach'.*

Notes

[1]See Mahmoud and Philip (2009) for a detailed review.

[2]See Kenny (2002; 2003) and Bedi (1999) for a detailed discussion.

[3]See Hofmann (2010) for detailed discussion.

[4]Internet regulation is basically restricting or controlling access to certain aspects or information.

[5]Laura Stein (2009) pinpoints internet's six functions for social movements: (a) providing information; (b) assisting action and mobilisation; (c) promoting interaction and dialogue; (d) making lateral linkage; (e) serving as an outlet for creative expression and (f) promoting fundraising and resource generation.

[6]In the literature, much of the focus of discussions on internet regulation has been on freedom of expression.

[7]Cited in Howard, Rheingold (1993). *The Virtual Community: Homesteading on the Electronic Frontiers,* MIT Press: Cambridge,7.

[8]Much of these activities/contents are illegal in most jurisdictions. As a matter of fact, in the recent past, cybercrime has been featured heavily in security news coverage and statistics are really very alarming.

[9]Although hate crime is punishable by law, but the boundary between hate crime and freedom of expression is not very clear.

[10]What is illegal varies from jurisdiction to jurisdiction and illegality is determined ultimately by the Courts in that jurisdiction. It is not a question of taste, individual judgement, culture or the age and background of those affected by the material (Department of Justic, Equality and Law Reform, 2010).. The ICMEC (International Centre for Mission and Exploited Children) study found that possession of child pornography is not a crime in 138 countries. In 122 countries, there is no law dealing with the use of computers and the Internet as a means of child porn distribution (Thomas 2006). In many countries child pornography is considered as obscene.

[11]There is a broad consensus in the literature that self regulation offers a number of benefits that can not be sufficiently achieved by the command and control approach of regulation Self regulation reduces the cost of implementation and compliance of state regulation. Further, it is more efficient in the sense that regulatory cost are not borne by the state.

[12]Also known as the "great Internet Sex Panic of 1995" was the first notable attempt by the US Congress to regulate pornographic material on the internet.

[13]The act excludes a few markets explicitly-certain fantasy sports bets are excluded, as are a number of skill games and any existing legal intrastate and inter-tribal gaming markets.

[14]See, Akdeniz (2001) for a detailed discussion.

[15]The Obscene Publications Act 1959 makes it illegal for websites that can be accessed from the UK without age restriction to contain certain types of adult content.

[16]The general benefits of self-regulation include efficiency, increased flexibility, increased incentives for compliance, and reduced cost.

[17]Internet filtering in Italy is applied against child pornography, gambling, and some P2P web-sites. The Pirate Bay website and IP Address are unreachable from Italy, blocked directly by Internet Service Providers.

[18]UK was first to introduce 'Internet Watch Foundation", an internet hotline service in 1996 to address harmful and illegal contents like child pornography and many other controversial contents.

[19]For details, visit http://www.inhope.org/gns/home.aspx

[20]Search engines also provide a possible framework through which harmful contents on the Internet can be limited. Search engine operations are generally based on keywords, with each system using a different approach to rank the search results requested by an end-user. It has been suggested that search engines could be effectively utilized to apply content rating frameworks such as PICS.

[21]For detailed discussion, please read 'Liability of Internet Service Providers (ISPs) and the exercise of freedom of expression in Latin America' by Claudio Ruiz Gallardo and J. Carlos Lara Gálvez (2011), accessed on http://www.palermo.edu/cele/english/publication.html

[22]See Goldsmith (2000) for a detailed discussion.

[23]The US and other developed countries had initially envisioned WSIS (World Summit on the Information Society) as an instrument to take forward their global 'digital opportunities' vision.

References

Akdeniz, Yaman (2001). Internet Content Regulation. *Computer Law and Security Report*. 17 (5): 303-317.

Anthony, Falzone (2013). Technology and Regulation. *Harvard Journal of Law and Public Policy.* 36 (1): 105-107.

Australian Classification Board (1995). *Classification of Material.* Accessed on https://en.wikipedia.org/wiki/Australian_Classification_Board

Australian Human Right Commission (2002) *"Internet Regulation in Australia",* Race Discrimination Unit, accessed on https://www.humanrights.gov.au/publications/internet-regulation-australia

Avgerou, C. (2001). The Significance of Context in Information Systems and Organisational Change. *Information Systems Journal* 11:43-63.

Bedi, A. (1999) The Role of Information and Communication Technologies-A Partial Survey, *ZEF Discussion Papers on Development Policy,* No. 7, Bonn.

Bessy C. & Brousseau E., (1997), *"The Governance of Intellectual Property Rights: Patents and Copyrights in France and in the US",* Inaugural Conference for The International Society for New Institutional Economics, The Present and Future of the New Institutional Economics , September 19-21, 1997, Washington University, St. Louis, Missouri, USA.

Borkar, Neha (2015). 11 Movies and Shows that Leaked on the Net before their Release. April 12, accessed on http://www.indiatimes.com/entertainment/celebs/11-movies-and-shows-that-leaked-on-the-net-before-their-release-231820.html?fb_comment_id=765000810282285_831211756994523#f33a8bd3f

Borkar, Neha (2015). 11 Movies and Shows that Leaked on the Net before their Release. Accessed on http://www.indiatimes.com/entertainment/celebs/11-movies-and-shows-that-leaked-on-the-net-before-their-release-231820.html

Chin, Josh (2015). China Internet Regulators Announce more Explicit Rules on Web Censorship. The Wall Street Journal, April 28.

Clark, Paul (2015). Desirable Accessory, Technology Solution or Fad?. OSC IB Blog. Accessed on http://blogs.osc-ib.com/2015/11/ib-teacher-blogs/dp_busman/desirable-accessory-technology-solution-or-fad/

COPA Commission (2000). *Key Recommendations of the Bertelsmann Foundation.* Accessed on http://www.copacommission.org/meetings/hearing3/machill.test.pdf

Daniel, Kennedy (2014). The Economic Impact of a Human Rights-Based Internet. Global Partners Digital, accessed on http://www.gp-digital.org/publication/economic-impact-of-a-human-rights-internet/

Department of Justic, Equality and Law Reform (2010).*Illegal and Harmful Use of Internet, First Report of the Working Group*, accessed on http://www.internetsafety.ie/website/ois/oisweb.nsf/0/77B7FDAED19CE22F802574C5004E587D/$File/working%20group%20repor%20on%20illegal%20and%20harmful%20use%20of%20the%20internet.pdf

Dutton, H. William ; Anna Dopatka; Michael Hills; Ginette Law and Victoria Nash (2010). *Freedom of Connection-Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet.* A report prepared for UNESCO's Division for Freedom of Expression, Democracy and Peace. Oxford Internet Institute. Accessed on http://portal.unesco.org/pv_obj_cache/pv_obj_id_4598876254B701E203952691673346E0E16C0E00/filename/UNESCO-19AUG10.pdf

EFA (2002). Internet Censorship: Law and Policy around the World. Electronic Frontiers Australia, accessed on https://www.efa.org.au/Issues/Censor/cens3.html

Electronic Frontiers Australia (2006), *''Internet Censorship Laws in Australia,''* March 31.

Elkin-Koren N. et Salzberger E.M., (1999) *"The Economic Analysis of Cyberspace :Challenges Posed by Cyberspace to Legal Theory and Legal Rules",* International Review of Law and Economics , Vol.19, pp. 553-582.

Ellison, L. And Akdeniz, Y. (1998). Cyber-stalking: the Regulation of Harassment on the Internet. Criminal Law Review, December Special Edition: Crime, Criminal Justice and the Internet, pp 29-48.

Eric, Pfanner (2011) *"Developing Country Want More Say in Internet Regulation",* New York Times, 28th June.

EuroISPA (2015). EuroISPA Highlights the Importance of Self Regulation in Ensuring a Safe Internet Environment. Accessed on http://www.euroispa.org/safer-internet-day-euroispa-highlights-importance-self-regulation-ensuring-safe-internet-environment/

Faisal, Irshaid (2014). How ISIS is Spreading its Message Online. *BBC Monitoring,* BBC News, June 19.

FCC (2016). *Children's Internet Protection Act.* Federal Communications Commission. Accessed on https://www.fcc.gov/consumers/guides/childrens-internet-protection-act

Geraldine Chin (2000) *''Technological Change and the Australian Constitution,''* Melbourne University Law Review, Vol. 25, No. 4.

Goldsmith, Jack (2000). Unilateral Regulation of the Internet: A Modest Defence. European Journal of International Law. 11 (1): 135-148.

Gütersloh (1999) *"Self Regulation of Internet Content",* Bertelsmann Foundation.

Hamelink, C.(2000) *The Ethics of Cyberspace,* Sage Publications: London.

Haris, Zargar (2013). India Must Wake up to Cyber Terrorism. Indo-Asian News Service. Accessed on http://gadgets.ndtv.com/internet/news/india-must-wake-up-to-cyber-terrorism-349274

Hill, Richard (2014). Human Rights, the Internet and its Governance. *Third World Resurgence*. No. 278-288: 40-41.

Hirst, David (2014). *Online Safety: Content Filtering by UK Internet Service Providers.* Science and Environment Section, Standard Note: SN 07031.

Hofmann, Jeanette (2010). The Libertarian Origin of Cybercrime: Unintended Side Effects of a Political Utopia. Discussion Paper 62. ESRC Research Centre, London School of Economics and Political Science.

Houng, K. Tan (2011). *Should the Internet Censorship be Imposed.* Accessed on https://wearticulate.wordpress.com/2011/04/18/cruelty-when-those-animals-get-abused/

Howard, Theresa (2009). Online Hate Speech: Difficult to Police…. And Define. US Today. Accessed on http://usatoday30.usatoday.com/tech/webguide/internetlife/2009-09-30-hate-speech_N.htm

IAMAI (2013). *India Must Wake up to the Cyber Terrorism.* The Times of India, accessed on http://www.iamai.in/media/details/1737

Iginio Gagliardone; Danit Gal; Thiago Alves and Gabriela Martinez (2015). Countering Online Hate Speech. United Nation Educational, Scientific and Cultural Organization: Paris.

ISPAI (2002). The Code and Practice and Ethics for the Internet Service Providers. The United Vpice of ISPs in Ireland, Accessed on http://www.ispai.ie/code-of-practice/

Jason Chan, Anindya Ghose, Robert Seamans. The Internet and Hate Crime: Offline Spillovers from Online Access. MIS Quarterly, September 2015 DOI: 10.2139/ssrn.2335637

Jawahitha Sarabdeen and María De-Miguel-Molina (2010). *Social network sites and protection of children: regulatory framework in Malaysia, Spain and Australia*. WSEAS Transactions on Computers 9(2):134-143.

Jeroen Van Laer and Peter Van Aelst (2010). Internet and Social Movement Action Repertories. *Information, Communication and Society.*13 (8): 1146-1171.

John, P. Hunter III (2013). *America the Sleeping Giant Must Awake.* Library of Congress: Washington, D.C.

Kalpan, Eben (2009). Terrorists and the Internet. Council on Foreign Relations, accessed on http://www.cfr.org/terrorism-and-technology/terrorists-internet/p10005

Kenneth, E. Himma and Herman, T. Tavani (2008). *The Handbook of Information and Computer Ethics.*. John Wiley & Sons: New Jersey.

Kenny, Charles (2003). The Internet and Economic Growth in Less Developed Countries: A Case of Managing Expectations. *Oxford Development Studies*. 31 (1): 99-113.Kenny, Charles. (2002) Information and communications technologies for direct poverty alleviation: costs and benefits, Development Policy Review. 20 (2): 141-157.

Kumar, Pradip (2014). Public Opinion on Censorship of Internet in India: A View from UP. Accessed on http://www.global.asc.upenn.edu/public-opinion-on-censorship-of-internet-in-india-a-view-from-up/

Kyle, McCarth (2015). Data Breaches Larger than Sony's in the Past Year. The Huffington Post. January 26.

London.

Mahapatra, Lisa (2014). Active Hate Groups in the US, and Here's Where they are. International Business Times. January 17, accessed on http://www.ibtimes.com/hate-group-map-there-are-1007-active-hate-groups-us-heres-where-they-are-map-1543623\

Mahmoud, E. Abd and Philip, J. Auter (2009). The Interactive Nature of Computer-Mediated Communication. *American Communication Journal.* 11 (4).

Manohar, Uttara (Retrieved March 2011) Pros and Cons of Internet Regulation. Retrieved from http://www.buzzle.com/articles/pros-and-cons-of-internet-regulation.html

Marie d'Udekem-Gevers and Yves Poullet (2002). *Internet Content Regulation: Concerns from a European User Empowerment Perspective about Internet Content Regulation: An Analysis of Some Recent Statements-Part II.* Computer Law and Security Review. 18 (1): 11-23.

MDA (2015). MDA's Approach to Regulating Content on Internet. Media Development Authority, Singapore Government. Accessed on http://www.mda.gov.sg/RegulationsAndLicensing/ContentStandardsAndClassification/Pages/Internet.aspx

Michael, S. (2008). Most Music Didn't Sell a Single Copy in 2008, *The Guardian,* 23 December.

Milgrom P., North D., Weingast B., (1990), *"The Role of Institutions in the Revival of Trade: The Law Merchant, Private Judges, and the Champagne Fairs",* Economics-and-Politics, Vol. 2, No.1 pp 1-23.

National Research Council (2001).*The Internet's Coming of Age,* National Academy Press: Washington, DC.

OpenNet Initiative, "China Tightens Controls on Internet News Content Through Additional Regulations," Bulletin 012, July 6, 2006 [online], http://www.opennet.net/bulletins/012/

Palme, Jacob (1998). Swedish Attempts to Regulate the Internet. Proceedings of IT'S Conference, accessed on http://people.dsv.su.se/~jpalme/society/swedish-attempts.html

Panos (1998). The Internet and Poverty. Panos Media Briefing, No. 28, Panos Institute,

Plumer, Brad. (2012). SOPA: How Much Does Online Piracy Really Cost the Economy? Washington Post. *The Washington Post,* 05 January.

Rikke, F. Jørgensen (2000-01). Internet and Freedom of Expression. European Master

Degree in Human Rights and Democratisation, Raoul Wellenberg Institute. Accessed on http://www.ifla.org/files/assets/faife/publications/ife03.pdf

Roger, Darlington (2009). How the Internet Could be Regulated. Presentation made at London School of Economics, accessed on http://www.rogerdarlington.me.uk/Internetregulation.html

Rose, Gregory (2012). Three Reasons why Internet Regulation is Necessary. Accessed on https://roseonpolitics.com/2012/04/28/three-reasons-why-internet-regulation-is-necessary/

Roy Jordan, (2002) ''*Free Speech and the Constitution,*'' Parliamentary Library, June 4, accessed on http://www.aph.gov.au/LIBRARY/Pubs/RN/2001-02/02rn42.htm.

Ruben, Enikolopove (2015). Does Social Media Promote Protests. *Free Political Series Brief.* CEFIR, November 23.

Spangler, Todd (2015). Top 20 Most Pirated Movies of 2014 Led by 'Wolf of Wall Street,' 'Frozen,' 'Gravity'" Variety. N.p., 28 December.

Srinath, Pavan (2015). Internet as a Public Goods: A Case of Net Neutrality. The Transitition State. Accessed on http://catalyst.nationalinterest.in/2015/04/19/internet-as-a-public-good-a-case-for-net-neutrality/

Stein, Laura (2009). Social Movement Web Use in Theory and Practice: A Content Analysis of US Movement Websites. New Media and Society. 11 (5): 749-777.

Sumanjeet (2006). E-Governance: An Overview in the India Context. *The Indian Journal of Political Science.* 67 (4): 857-866.

Sumanjeet (2008). Impact of E-Commerce on Economic Models: Little to Lose; More to Gain. *International Journal of Trade and Global Markets*. 1(3): 319-337.

Sweney, M. 2011. Global Recorded Music Sales Fall Almost $1.5bn Amid Increased Piracy, The Guardian, 28th March.

The Culturiest (2013) *"More than 2 Billion People use the Internet. Here is What they are up to (Infographics)"* accessed on http://www.thecultureist.com/2013/05/09/how-many-people-use-the-internet-more-than-2-billion-infographic/

The Guardian (2012). *Battle the Internet.* Accessed on https://www.theguardian.com/technology/datablog/2012/apr/16/internet-censorship-country-list

Thomas, Claburn (2006). Study: Child Porn isn't Illegal in Most Countries. Informationweek. June 4. Accessed at http://www.informationweek.com/study-child-porn-isnt-illegal-in-most-countries/d/d-id/1042033?

Uaddit (2010). Net Neutrality Legislations: Pros and Cons?, accessed on http://uaddit.com/discussions/showthread.php?t=15417

UNHR (2011). Freedom of Expression Everywhere, Including in Cyberspace. United Nations Human Rights, accessed on http://www.ohchr.org/EN/NewsEvents/Pages/Freedomofexpressioneverywhere.aspx

USLegal (2009). Laws Regulating Privacy on the Internet. Accessed on http://internetlaw.uslegal.com/regulation/privacy/laws-regulating-privacy-on-the-internet/

Walsham, G. (1993). The Emergence of Interpretivism in IS Research. *Information Systems Research* 6(4): 376-394.

Williams, Rhiannon (2014). Cybercrime Costs Global Economy $ 445 billion Annually. The Telgraph. June 9. Accessed on http://www.telegraph.co.uk/technology/internet-security/10886640/Cyber-crime-costs-global-economy-445-bn-annually.html

World CP (2014). India/ 4.2: Recent Policy Issues and Debates. Accessed on http://www.worldcp.org/india.php?aid=426

Yaman, Akdeniz (2002) *"Internet Content Regulation: UK government and the Control of Internet Content",* Computer Law and Security Report, 17 (5): 303-317.

Dr. Sumanjeet Singh is an assistant professor in the Department of Commerce at Ramjas College, University of Delhi, India. He has been awarded with "*Rashtriya Vidhya Sarswati"* Award and *"Rajiv Gandhi Excellence Award",* 2008 for his outstanding contribution in the field of application of ICTs and e-commerce. His areas of interest are Internet studies, development issues, law and economics.